

DII COE

Security Checklist

Version 2.0

27 June 1997

SECTION 1

Introduction

Background

The Defense Information Infrastructure (DII) is a defense-level enterprise effort to develop and field military systems that will meet the needs of the warfighter in a global information environment. The DII addresses systems in the command and control, intelligence, and combat support domains within the Department of Defense (DOD). The DII Common Operating Environment (COE) provides a distributed application infrastructure that promotes interoperability, portability, and scalability DOD-wide. The objective of the DII COE is to provide access to data, independent of location, in a secure, reliable, cost-efficient manner. The DII COE provides an open system foundation for the development of mission-critical systems like the Global Command and Control System (GCCS) and the Global Combat Support System (GCSS).

Purpose

This document provides the DII COE community with a number of information systems security (INFOSEC) checklists. The checklists were prepared for the DII COE independent of the manner in which the COE may be used in the GCCS or the GCSS. The GCCS, GCSS, and other systems will supplement the security features of the DII COE in areas outside the scope of the DII COE (e.g., network security).

The primary audience for most of this document is the COE kernel developer. However, system developers should understand the security configuration of the COE and take actions appropriate for their roles. System developers should use the checklist to ensure that during the development process they have not reduced the strength of the security provided by the COE.

Certification and accreditation authorities can use the checklists to develop security test and evaluation plans and procedures. Detailed test steps are included for use by checklist users to determine if security objectives have been met.

Variation from the specified values and configurations should not be made without first performing a security risk assessment.

Scope

A checklist includes security-relevant practices and precautions applicable to a DII COE component. This document includes a checklist for DII COE operating systems, database management systems (DBMS), the Distributed Computing Environment (DCE), and applications security checklist.

Document Organization

Except for the applications security checklist, each checklist is organized by topic and subtopics. For each subtopic, a security objective and rationale for meeting that objective are stated where applicable. *DII COE Security Software Requirements Specification(SRS)* requirements that apply to the security objective are also presented. Following the SRS requirement, test actions are included for determining if the objective is met. These actions include one or more steps. For each step, the required action, expected results, and applicable comments are included.

The applications security checklist presents security guidance for use by application developers. This checklist provides a guidance statement and rationale for implementing the guidance. The checklist is in tabular format.

The checklists have been entered in a database and checklists have been produced using the report generation capability of a database management system (DBMS). The DBMS used is Microsoft Access. The checklists are given in appendixes. This document includes the following appendixes:

- A: Solaris 2.4 Security Checklist
- B: HP-UX 10.x Security Checklist
- C: Microsoft Windows NT 3.51 Security Checklist
- D: SYBASE Security Checklist
- E: Oracle Security Checklist
- F: Informix Security Checklist
- G: DCE Security Checklist
- H: Applications Security Checklist
- I: Solaris 2.5.1 Security Checklist
- J: Microsoft Windows NT 4.0 Security Checklist

Information Sources

Information in this document is derived from the following sources:

The MITRE Corporation, *Security Test and Evaluation Plan for the Global Command and Control System (GCCS) Leading Edge Services (LES)*, January 1996.

Australian Computer Emergency Response Team (AUSCERT), *Unix Computer Security Checklist*, v1.1,
ftp://ftp.auscert.org.au/pub/auscert/papers/unix_security_checklist, 19 December 1995.

Defense Intelligence Agency, *Department of Defense Intelligence Information System (DODIIS) Security Architecture Guidance and Directions (Draft)*, June 1995.

Garfinkel, Simson, and Gene Spafford, *Practical UNIX Security*, O'Reilly & Associates, Inc., October 1992.

The MITRE Corporation, *DII COE Software Security Requirements Specification (SRS)*, Version 1.2, 1 December 1995.

Solaris 2.4 documentation.

HP-UX 10.1 documentation.

Oracle documentation.

Sybase documentation.

Informix documentation.

Somarsoft Corporation, *Windows NT Security Issues*,
<http://www.somarsoft.com/security.htm>

Less Well-Known Considerations for Configuring a Secure Windows NT System,
Mayer, Frank L., SAIC, 29 March 1996.

Microsoft Corporation, *Microsoft Windows NT Version 3.5, Administrator's Security Guide*.

Solaris 2.5.1 documentation

Microsoft Corporation, *Microsoft Windows NT Version 4.0, Administrator's Security Guide*.